# Die Erzeugenden der Hauptkongruenzgruppen für Primzahlstufen

INAUGURAL-DISSERTATION

zur

Erlangung der Doktorwürde

einer

Hohen Naturwissenschaftlichen Fakultät

der

Eberhard-Karls-Universität zu Tübingen

vorgelegt

von

Hermann Frasch

aus Stuttgart

Dekan der Fakultät: Prof. Dr. Machatschki.

Berichterstatter: Prof. Dr. Knopp.

Tag der mündlichen Prüfung: 21. Juli 1932.

R. UNIV.
BIBLIOTHEEK
LEIDEN

Druck: Dr. Karl Höhn, Tübingen.

## Einleitung.

Erzeugende der Hauptkongruenzgruppen hat bis $p = 7$ Klein[1]) angegeben auf Grund der Ränderzuordnung ihrer Fundamentalbereiche, wenn diese aufgefaßt werden als die die zugehörigen Modulargruppen repräsentierenden Teile der Modulteilung der positiven Halbebene. Dieses Verfahren ist geometrisch anschaulich und darum zunächst auf kleine Stufenzahlen beschränkt. Im folgenden werden diese Erzeugenden rein gruppentheoretisch bestimmt mit Hilfe des allgemeinen von Reidemeister[2]) und Schreier[3]) stammenden Verfahrens, welches erlaubt, Untergruppen von Gruppen, die durch Erzeugende und Relationen zwischen diesen definiert sind, auf ebensolche Weise zu definieren. Es scheint nun, daß dabei eine in gewissem Sinne einfache Wahl der Nebengruppenrepräsentanten (Elemente der Modulargruppe) mit einer Komplizierung des durch die sich einstellenden Relationen geforderten Eliminationsverfahrens Hand in Hand geht. Die Repräsentanten werden daher im Interesse eines im allgemeinen Fall sehr glatten und durchsichtigen Eliminationsverfahrens gewählt. Im übrigen zeigt der Gang der Untersuchung naturgemäß große Analogie zu einer Arbeit von Rademacher[4]), in der die durch $c \equiv 0 \pmod{p}$ gegebenen Untergruppen vom Index $p + 1$ auf dieselbe Weise behandelt werden. Das Resultat von Rademacher läßt sich daher auch aus unserem (§ 6) ableiten.

In § 7 wird die Anzahl der freien Erzeugenden bestätigt durch einen allgemeineren Satz über Erzeugendenanzahlen von gewissen Untergruppen

---

[1]) Klein-Fricke, „Elliptische Modulfunktionen", Bd. 1.

[2]) K. Reidemeister, „Knoten und Gruppen" (§ 1), Hambg. Abh. 5, S. 6.

[3]) O. Schreier, „Die Untergruppen der freien Gruppen", ebenda, S. 161.

[4]) H. Rademacher, „Über die Erzeugenden von Kongruenzuntergruppen der Modulgruppe", Hambg. Abh. 7, S. 134.

freier Produkte zyklischer Gruppen. Er ist als Verallgemeinerung einer von Schreier[5]) für freie Gruppen aufgestellten Beziehung anzusehen. Daran anschließend wird zum selben Zweck eine geometrisch-topologische Interpretation durchgeführt. In § 8 wird das gewonnene Resultat zur abstrakten Charakterisierung der Modulargruppe benutzt.

## § 1.

## Die Modulargruppe.

Die inhomogene Modulgruppe wird erzeugt durch die beiden Substitutionen

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ und } T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \tag{1}$$

die den Relationen

$$T^2 = (TS)^3 = 1 \tag{2}$$

genügen. In ihr bilden die Substitutionen $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit

$$a \equiv d \equiv 1, \quad b \equiv c \equiv 0 \pmod{p} \tag{3}$$

einen Normalteiler $\Gamma_p$, die „Hauptkongruenzgruppe $p$-ter Stufe". Ihre Faktorgruppe $\mathfrak{G}_g^{(p)}$, die „Modulargruppe $p$-ter Stufe", besteht aus den mod $p$ miteinander inkongruenten Substitutionen, deren Anzahl sich zu $g = \frac{1}{2} p (p^2 - 1)$ bestimmt. Sie gelten als Repräsentanten der Nebengruppen von $\Gamma_p$; man kann sie nach v. Dyck[6]) durch

$$\begin{matrix} V^\lambda S^\mu \\ V^\lambda S^\mu T S^\nu \end{matrix} \tag{4}$$

$$\lambda = 0, 1, \ldots, \tfrac{1}{2}(p-3); \quad \mu = 0, 1, \ldots, p-1; \quad \nu = 0, 1, \ldots, p-1 \tag{5}$$

darstellen. Dabei ist, wenn wir wie im folgenden $p > 3$ annehmen,

$$V = T S^\alpha T S^\beta T S^\alpha, \tag{6}$$

wo $\alpha$ eine primitive Wurzel von $p$, und $\beta$ so bestimmt ist, daß $\alpha\beta \equiv 1 \pmod{p}$. Ausgerechnet bedeutet $V$ die Substitution

$$\begin{pmatrix} -\beta & 1-\alpha\beta \\ \alpha\beta - 1 & -\alpha + \alpha(\alpha\beta - 1) \end{pmatrix},$$

ist also mit $\begin{pmatrix} \beta & 0 \\ 0 & \alpha \end{pmatrix}$ kongruent und hat daher die Ordnung $\frac{1}{2}(p-1)$. Denn man hat

$$V^\lambda \equiv T S^{\alpha^\lambda} T S^{\beta^\lambda} T S^{\alpha^\lambda} \equiv \begin{pmatrix} \beta^\lambda & 0 \\ 0 & \alpha^\lambda \end{pmatrix} \pmod{p}. \tag{7}$$

---

[5]) a. a. O., § 4.

[6]) v. Dyck, „Gruppentheoretische Studien", Math. Ann. 20 (1882), S. 41 f.

Ebenso findet man

$$V^\lambda S^\mu \equiv \begin{pmatrix} \beta^\lambda & \mu\,\beta^\lambda \\ 0 & \alpha^\lambda \end{pmatrix}$$

$$V^\lambda S^\mu T S^\nu \equiv \begin{pmatrix} \mu\,\beta^\lambda & (\mu\,\nu - 1)\,\beta^\lambda \\ \alpha^\lambda & \nu\,\alpha^\lambda \end{pmatrix} \pmod p. \tag{8}$$

Man ersieht aus diesen Darstellungen, daß die Elemente (4) alle voneinander verschieden sind und gerade $\frac{1}{2}p(p^2-1)$ Elemente ausmachen.

Um die Kompositionsverhältnisse von $\mathfrak{G}^{(p)}$ zu kennen, genügt es offenbar, festzustellen, in welches andere Element ein Element aus (4) bei rechtsseitiger Multiplikation mit $S$, $T$ oder $V$ übergeht. Die Komposition mit $S$ ist trivial, ebenso diejenige mit $T$ bei dem ersten Teil der Elemente (4). Dagegen gilt:

$$V^\lambda S^\mu T S^\nu \cdot T \equiv V^{\lambda_*} S^{\mu_*} T S^{\nu_*} \qquad \nu \not\equiv 0 \pmod p, \tag{9}$$

wobei

$$\begin{aligned} \lambda_* &\equiv \lambda + \overset{\alpha}{\operatorname{ind}}\,\nu && \left(\bmod \frac{p-1}{2}\right), \\ \mu_* &\equiv \mu\,\nu^2 - \nu && (\bmod p), \\ \nu\,\nu_* &\equiv -1 && (\bmod p). \end{aligned} \tag{10}$$

Der Beweis ergibt sich durch Vergleich von

$$V^\lambda S^\mu T S^\nu T \equiv \begin{pmatrix} \mu\,\beta^\lambda & (\mu\,\nu-1)\,\beta^\lambda \\ \alpha^\lambda & \nu\,\alpha^\lambda \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} (\mu\,\nu-1)\,\beta^\lambda & -\mu\,\beta^\lambda \\ \nu\,\alpha^\lambda & -\alpha^\lambda \end{pmatrix}$$

und

$$V^{\lambda_*} S^{\mu_*} T S^{\nu_*} \equiv \begin{pmatrix} \mu_*\,\beta^\lambda & (\mu_*\,\nu_* - 1)\,\beta^{\lambda_*} \\ \alpha^{\lambda_*} & \nu_*\,\alpha^{\lambda_*} \end{pmatrix}.$$

Da nun mod $p$

$$\begin{aligned} \mu_*\,\beta^{\lambda_*} &\equiv \pm(\mu\,\nu^2 - \nu)\,\beta^{\lambda + \operatorname{ind}\nu} \\ &\equiv \pm\nu\,\beta^{\operatorname{ind}\nu}(\mu\,\nu - 1)\,\beta^\lambda \\ &\equiv \pm(\mu\,\nu - 1)\,\beta^\lambda, \\ (\mu_*\,\nu_* - 1)\,\beta^{\lambda_*} &\equiv \pm[\nu(\mu\,\nu - 1)\,\nu_* - 1]\,\beta^{\lambda + \operatorname{ind}\nu} \\ &\equiv \mp\mu\,\nu\,\beta^{\lambda + \operatorname{ind}\nu} \\ &\equiv \mp\mu\,\beta^\lambda, \\ \alpha^{\lambda_*} &\equiv \pm\alpha^{\lambda + \operatorname{ind}\nu} \\ &\equiv \pm\nu\,\alpha^\lambda, \\ \nu_*\,\alpha^{\lambda_*} &\equiv \pm\nu_*\,\nu\,\alpha^\lambda \\ &\equiv \mp\alpha^\lambda, \end{aligned}$$

wo entweder nur das obere oder nur das untere Vorzeichen gilt [im Fall der homogenen Modulgruppe wäre $\lambda$ und $\lambda_*$ mod $(p-1)$ zu nehmen, so daß das obere Zeichen gelten müßte], so ist die Richtigkeit von (9) nachgewiesen.

Mit Hilfe von (9) findet man:

$$V^{\lambda} S^{u} \cdot V = V^{\overline{\lambda+1}} S^{\overline{u\alpha^2}} \pmod{p}, \tag{11}$$

$$V^{\lambda} S^{u} T S^{v} \cdot V = V^{\overline{\lambda-1}} S^{\overline{u\beta^2}} T S^{\overline{v\alpha^2}} \pmod{p}. \tag{12}$$

Dabei sind die Exponenten von $V$ mod $\frac{1}{2}(p-1)$, die von $S$ mod $p$ zu reduzieren. Das sei durch die Striche angedeutet.

Aus (11) folgt übrigens, daß die $V$ und $S$ eine Untergruppe vom Index $p+1$ erzeugen.

## § 2.

### Die Erzeugenden der Hauptkongruenzgruppen.

Um die Erzeugenden von $\Gamma_p$ angeben zu können, haben wir nach dem Verfahren von Schreier folgende Ausdrücke zu bilden:

$$U_{\overline{G},X} = \overline{G} X \overline{G X}^{-1}. \tag{13}$$

Durchläuft dabei $\overline{G}$ sämtliche Repräsentanten der Nebengruppen von $\Gamma_p$, also die Elemente (4), und $X$ die Erzeugenden der Modulgruppe, so stellt (13) die Gesamtheit der Erzeugenden von $\Gamma_p$ vor. Die Relationen, denen die $U$ noch gehorchen, werden besonders einfach, wenn die $\overline{G}$ die Schreiersche Bedingung $(F)$ erfüllen, die besagt, daß mit jedem $\overline{G}$ auch $\overline{G}X^{-1}$ ein Nebengruppenrepräsentant sein soll, wenn in dem „Wort" $\overline{G}$ der letzte „Buchstabe" $X$ heißt. Allgemein ist durch $(F)$ im Sinne der Klein-Dyckschen geometrischen Interpretation einfacher Zusammenhang des Fundamentalbereichs der betrachteten Untergruppe gefordert. Zerfällt der Fundamentalbereich in $t$ diskrete Teile, so folgt aus der Schreierschen Herleitung, daß zu den Relationen, die den Relationen der Obergruppe und ihren Transformationen entsprechen, noch $t-1$ weitere Relationen treten. Diese bilden sozusagen die „Ketten" zwischen den diskreten Teilen. In unserem Falle sind gerade $\frac{1}{2}(p-1)$ Teile vorhanden. Geht man davon aus, daß jedem Teil gerade einer der rationalen Punkte $V^{\lambda}(\infty)$ zugehört, so ist es nicht schwer, sich ein Bild von der Gestalt des gewählten Fundamentalbereichs zu machen.

Da die Elemente (4) also wegen der Bedeutung von $V$ die Bedingung $(F)$ nicht erfüllen, so kann man, wenn man die getroffene Wahl der Repräsentanten beibehalten will, sich damit helfen, daß man die Modulgruppe als von den drei Elementen $S$, $T$ und $V$ erzeugt ansieht, muß dann aber die weitere Relation

$$T S^{\alpha} T S^{\beta} T S^{\alpha} V^{-1} = 1$$

in Kauf nehmen.

In (13) sind dann folgende Erzeugende inbegriffen:

1. $U_{\lambda,\mu,S} = V^\lambda S^{\mu+1} \overline{V^\lambda S^{\mu+1}}^{-1}$.

Diese Erzeugenden sind mit der Einheit identisch außer für $\mu = p-1$:

$$U_{\lambda,p-1,S} = V^\lambda S^p V_{\infty}^{-\lambda}.$$

2. $U_{\lambda,\mu,\nu,S} = V^\lambda S^\mu T S^{\nu+1} \overline{V^\lambda S^\mu T S^{\nu+1}}^{-1}$.

Auch hier bleibt nur übrig

$$U_{\lambda,\mu,p-1,S} = V^\lambda S^\mu T S^p T^{-1} S^{-\mu} V^{-\lambda}.$$

3. $U_{\lambda,\mu,T} = V^\lambda S^\mu T \overline{V^\lambda S^\mu T}^{-1} \equiv 1.$

4. $U_{\lambda,\mu,\nu T} = V^\lambda S^\mu T S^\nu T \overline{V^\lambda S^\mu T S^\nu T}^{-1}$.

Gemäß (9) ist also

$$U_{\lambda,\mu,0,T} = V^\lambda S^\mu T^2 S^{-\mu} V^{-\lambda}$$

und

$$U_{\lambda,\mu,\nu,T} = V^\lambda S^\mu T S^\nu T S^{-\nu_*} T^{-1} S^{-\mu_*} V^{-\lambda_*} \qquad \nu \neq 0.$$

5. $U_{\lambda,\mu,V} = V^\lambda S^\mu V \overline{V^\lambda S^\mu V}^{-1}$.

Unter ihnen ist nach (11)

$$U_{\lambda,0,V} \equiv 1 \qquad \lambda \neq \frac{p-3}{2},$$

$$U_{\frac{p-3}{2},0,V} = V^{\frac{p-1}{2}},$$

$$U_{\lambda,\mu,V^\alpha} = V^\lambda S^\mu V S^{-\overline{\mu\alpha^2}} V^{-\overline{\lambda+1}} \qquad \mu \neq 0.$$

Schließlich ist nach (12)

6. $U_{\lambda,\mu,\nu,V} = V^\lambda S^\mu T S^\nu V \overline{V^\lambda S^\mu T S^\nu V}^{-1}$

$$= V^\lambda S^\mu T S^\nu V S^{-\overline{\nu\alpha^2}} T^{-1} S^{-\overline{\mu\beta^2}} V^{-\overline{\lambda-1}}.$$

## § 3.

## Die Relationen der Erzeugenden.

Zwischen den aufgestellten Erzeugenden bestehen nun folgende Relationen:

(14) $$\overline{G} T^2 \overline{G}^{-1} = 1,$$

(15) $$\overline{G} (TS)^3 \overline{G}^{-1} = 1,$$

(16) $$\overline{G} T S^\alpha T S^\beta T S^\alpha V^{-1} \overline{G}^{-1} = 1.$$

Sie sind so zu verstehen, daß ihre linken Seiten durch die $U$ ausgedrückt werden sollen. Wir schreiben sie daher ausführlich:

(14a) $$R_1 = V^\lambda S^\mu T^2 S^{-\mu} V^{-\lambda} = 1,$$

(14b) $$R_2 = V^\lambda S^\mu T S^\nu T^2 S^{-\nu} T^{-1} S^{-\mu} V^{-\lambda} = 1,$$

(15a) $$R_3 = V^\lambda S^\mu T S T S T S^{1-\mu} V^{-\lambda} = 1,$$

(15b) $$R_4 = V^\lambda S^\mu T S^\nu T S T S T S^{1-\nu} T^{-1} S^{-\mu} V^{-\lambda} = 1,$$

(16a) $$R_5 = V^\lambda S^\mu T S^\alpha T S^\beta T S^\alpha V^{-1} S^{-\mu} V^{-\lambda} = 1,$$

(16b) $$R_6 = V^\lambda S^\mu T S^\nu T S^\alpha T S^\beta T S^\alpha V^{-1} S^{-\nu} T^{-1} S^{-\mu} V^{-\lambda} = 1.$$

(14a) ergibt

$$R_1 = U_{\lambda,\mu,0,T} = 1.$$

Dagegen gibt (14b) zu einer wesentlichen Relation Anlaß:

(17) $$R_2 = V^\lambda S^\mu T S^\nu T^{-1} S^{-\nu_*} T S^{-\mu_*} V^{-\lambda_*} V^{\lambda_*} S^{\mu_*} T S^{\nu_*} T S^{-\nu} T^{-1} S^{-\mu} V^{-\lambda}$$
$$= U_{\lambda,\mu,\nu,T} U_{\lambda_*,\mu_*,\nu_*,T} = 1.$$

Denn es gelten die Beziehungen:

(18) $$\lambda_{**} = \lambda, \quad \mu_{**} = \mu, \quad \nu_{**} = \nu.$$

(15a) liefert, wobei wie weiterhin (14a) bereits berücksichtigt wird:

(19) $$R_3 = V^\lambda S^\mu T S T S S^{-p} T^{-1} S^{-\mu+1} V^{-\lambda} V^\lambda S^{\mu-1} T S^p T S^{1-\mu} V^{-\lambda}$$
$$= U_{\lambda,\mu,1,T} U_{\lambda,\mu-1,p-1,S} = 1, \text{ wenn } \mu \neq 0.$$

Für $\mu = 0$ jedoch:

(20) $$R_3 = V^\lambda T S T S T S V^{-\lambda}$$
$$= V^\lambda T S T S S^{-p} T S^{-(p-1)} V^{-\lambda} V^\lambda S^{p-1} T S^p T S V^{-\lambda}$$
$$= U_{\lambda,0,1,T} U_{\lambda,p-1,p-1,S} V^\lambda S^{p-1} S V^{-\lambda}$$
$$= U_{\lambda,0,1,T} U_{\lambda,p-1,p-1,S} U_{\lambda,p-1,S} = 1.$$

Wir kommen zu (15b). Nehmen wir zunächst $\nu = 0$ an, so ist

$$R_4 = V^\lambda S^\mu T^2 S T S T S T S^{-\mu} V^{-\lambda} = 1.$$

Diese Relation führt nach kurzer Rechnung auf (19) und (20) zurück, besagt also nichts Neues. Dasselbe gilt für $\nu = 1$. Wir setzen daher $\nu \neq 0, \neq 1$ und können dann folgende bemerkenswerte Rechnung durchführen:

$$R_4 = V^\lambda S^\mu T S^\nu T S T S T S^{1-\nu} T^{-1} S^{-\mu} V^{-\lambda}$$
$$= U_{\lambda,\mu,\nu,T} V^{\lambda_*} S^{\mu_*} T S^{\nu_*} S T S T S^{1-\nu} T^{-1} S^{-\mu} V^{-\lambda}.$$

Setzen wir $\lambda_1 = \lambda_*$, $\mu_1 = \mu_*$, $\nu_1 = \nu_* + 1$, so können wir weiter schreiben:

$$R_4 = U_{\lambda,\mu,\nu,T} U_{\lambda_1,\mu_1,\nu_1,T} V^{\lambda_{1*}} S^{\mu_{1*}} T S^{\nu_{1*}} S T S^{1-\nu} T^{-1} S^{-\mu} V^{-\lambda}.$$

Wir setzen wieder $\lambda_2 = \lambda_{1*}$, $\mu_2 = \mu_{1*}$, $\nu_2 = \nu_{1*} + 1$, so daß

$$R_4 = U_{\lambda,\mu,\nu,T} U_{\lambda_1,\mu_1,\nu_1,T} U_{\lambda_2,\mu_2,\nu_2,T} V^{\lambda_{2*}} S^{\mu_{2*}} T S^{\nu_{2*}+1-\nu} T^{-1} S^{-\mu} V^{-\lambda}.$$

Nimmt man noch $\lambda_3 = \lambda_{2*}$, $\mu_3 = \mu_{2*}$, $\nu_3 = \nu_{2*} + 1$, so ist es eine rein gruppentheoretische Folge, daß $\lambda_3 = \lambda$, $\mu_3 = \mu$, $\nu_3 = \nu$. Der eben angegebene Prozeß der Erzeugung der Zahlentripel $\lambda, \mu, \nu$ auseinander hat also die Periode 3. Wir wollen das noch zahlentheoretisch nachweisen.

Nach (10) ist:

$$\begin{aligned} \nu\,(\nu_1 - 1) &\equiv -1 \pmod p \\ \nu_1(\nu_2 - 1) &\equiv -1 \\ \nu_2(\nu_3 - 1) &\equiv -1 \end{aligned}$$

$$\begin{aligned} \nu\ \nu_1 &\equiv -1 \\ \nu_1\,\nu_2 &\equiv -1 \\ \nu_2\,\nu_3 &\equiv -1 \end{aligned}$$

$$\begin{aligned} \nu_2\,\nu_3\,(\nu_1 - 1) &\equiv \nu_1\,\nu_2\,(\nu_2 - 1) \\ \nu_3\,(\nu_1 - 1) &\equiv -1, \end{aligned}$$

folglich

$$\nu_3 = \nu.$$

$$\begin{aligned} \mu_1 = \mu_* &\equiv \mu\,\nu^2 - \nu \pmod p \\ \mu_2 = \mu_{1*} &\equiv (\mu\,\nu^2 - \nu)\,\nu_1^2 - \nu_1 \\ &\equiv \mu\,\nu^2\,\nu_1^2 - \nu\,\nu_1 - \nu_1 \\ &\equiv \mu\,(\nu - 1)^2 - (\nu - 1)\,\nu_1 - \nu_1 \\ &\equiv \mu\,(\nu - 1)^2 - (\nu - 1) \\ \mu_3 = \mu_{2*} &\equiv \mu_2\,\nu_2^2 - \nu_2 \\ &\equiv (\nu - 1)\,(\mu\,(\nu - 1) - 1)\,\nu_2^2 - \nu_2 \\ &\equiv -\mu\,(\nu - 1)\,\nu_2 + \nu_2 - \nu_2, \end{aligned}$$

folglich

$$\mu_3 = \mu.$$

Schließlich ist

$$\begin{aligned} \lambda_1 &\equiv \lambda + \operatorname{ind}\nu \pmod{\frac{p-1}{2}} \\ \lambda_2 &\equiv \lambda + \operatorname{ind}\nu + \operatorname{ind}\nu_1 \\ &\equiv \lambda + \operatorname{ind}(\nu - 1) \\ \lambda_3 &\equiv \lambda + \operatorname{ind}(\nu - 1) + \operatorname{ind}\nu_2 \\ &\equiv \lambda + \operatorname{ind}(-1), \end{aligned}$$

woraus

$$\lambda_3 = \lambda.$$

Die letzte Rechnung macht deutlich, warum die Fälle $\nu = 0$ und $\nu = 1$ hier nicht subsumiert werden konnten. Man bestätigt leicht, daß auch $\nu_1$ und $\nu_2$ diese Werte nicht annehmen.

Die aus (15b) gefundene Relation lautet nunmehr:

(21) $$U_{\lambda,\mu,\nu,T}\,U_{\lambda_1,\mu_1,\nu_1,T}\,U_{\lambda_2,\mu_2,\nu_2,T} = 1.$$

## § 4.

## Weitere Relationen.

Die Relationen (16), denen wir uns jetzt zuwenden, werden unter anderem dazu dienen, die unechten Erzeugenden $U_V$, die ja nur auftreten, weil wir $V$ als Erzeugende der Modulgruppe anerkannt haben, durch die $U_S$ und $U_T$ auszudrücken. Daß in ihnen aber auch noch weitere wesentliche Relationen, nämlich die „Ketten"-Relationen, enthalten sind, folgt z. B. auch aus der Tatsache, daß einige der $U_{\lambda,\mu,V}$ mit der Einheit identisch sind.

Wir beginnen bei (16a) mit dem Fall $\mu = 0$, $\lambda \neq \frac{p-3}{2}$:

$$
\begin{aligned}
(22) \qquad R_5 &= V^\lambda T S^\alpha T S^\beta T S^\alpha V^{-1-\lambda} \\
&= U_{\lambda,0,\alpha,T} V^{\lambda+1} S^{p-\alpha} T S^{p-\beta} S^\beta T S^\alpha V^{-1-\lambda} \\
&= U_{\lambda,0,\alpha,T} U_{\lambda+1,p-\alpha,p-1,S} V^{\lambda+1} S^{p-\alpha} S^\alpha V^{-1-\lambda} \\
&= U_{\lambda,0,\alpha,T} U_{\lambda+1,p-\alpha,p-1,S} U_{\lambda+1,p-1,S} = 1 \qquad \lambda \neq \frac{p-3}{2}.
\end{aligned}
$$

Damit sind die noch ausstehenden Relationen bereits gefunden, jedoch seien der Vollständigkeit halber die etwas umständlichen Eliminationsrelationen der $U_V$ sämtlich aufgestellt.

Es sei also $\mu = 0$, $\lambda = \frac{p-3}{2}$:

$$
\begin{aligned}
(23) \qquad R_5 &= V^{\frac{p-3}{2}} T S^\alpha T S^\beta T S^\alpha V^{-\frac{p-1}{2}} \\
&= U_{\frac{p-3}{2},0,\alpha,T} S^{p-\alpha} T S^{p-\beta} S^\beta T S^\alpha V^{-\frac{p-1}{2}} \\
&= U_{\frac{p-3}{2},0,\alpha,T} U_{0,p-\alpha,p-1,S} S^{p-\alpha} S^\alpha V^{-\frac{p-1}{2}} \\
&= U_{\frac{p-3}{2},0,\alpha,T} U_{0,p-\alpha,p-1,S} U_{0,p-1,S} U^{-1}_{\frac{p-3}{2},0,V} = 1.
\end{aligned}
$$

Für $\mu \not\equiv 0$ findet man:

$$
\begin{aligned}
(24) \qquad R_5 &= V^\lambda S^\mu T S^\alpha T S^\beta T S^\alpha V^{-1} S^{-\mu} V^{-\lambda} \\
&= U_{\lambda,\mu,\alpha,T} V^{\overline{\lambda+1}} S^{\overline{\mu\alpha^2-\alpha}} T S^{p-\beta} S^\beta T S^\alpha V^{-1} S^{-\mu} V^{-\lambda} \\
&= U_{\lambda,\mu,\alpha,T} U_{\overline{\lambda+1},\overline{\mu\alpha^2-\alpha},p-1,S} V^{\overline{\lambda+1}} S^{\overline{\mu\alpha^2-\alpha}} S^\alpha V^{-1} S^{-\mu} V^{-\lambda} \\
&= U_{\lambda,\mu,\alpha,T} U_{\overline{\lambda+1},\overline{\mu\alpha^2-\alpha},p-1,S} U^{\varepsilon}_{\overline{\lambda+1},p-1,S} U^{-1}_{\lambda,\mu,V} = 1.
\end{aligned}
$$

Dabei ist $\varepsilon = 0$ oder 1, je nachdem $\overline{\mu\alpha^2-\alpha} + \alpha \lesseqgtr p$.

Jetzt steht noch (16b) aus. Zunächst sei $\nu = 0$:

$$(25)\quad R_6 = V^{\lambda} S^{\mu+\alpha} T S^{\beta} T S^{\alpha} V^{-1} T^{-1} S^{-\mu} V^{-\lambda}$$
$$= U^{\varepsilon}_{\lambda,\, p-1,\, S} U_{\lambda,\, \overline{\mu+\alpha},\, \beta,\, T} V^{\overline{\lambda-1}} S^{\overline{\mu\beta^2}} T S^{p-\alpha} S^{\alpha} V^{-1} T^{-1} S^{-\mu} V^{-\lambda}$$
$$= U^{\varepsilon}_{\lambda,\, p-1,\, S} U_{\lambda,\, \overline{\mu+\alpha},\, \beta,\, T} U_{\overline{\lambda-1},\, \overline{\mu\beta^2},\, p-1,\, S} V^{\overline{\lambda-1}} S^{\overline{\mu\beta^2}} T V^{-1} T^{-1} S^{-\mu} V^{-\lambda}$$
$$= U^{\varepsilon}_{\lambda,\, p-1,\, S} U_{\lambda,\, \overline{\mu+\alpha},\, \beta,\, T} U_{\overline{\lambda-1},\, \overline{\mu\beta^2},\, p-1,\, S} U^{-1}_{\lambda,\, \mu,\, 0,\, V} = 1.$$

Dabei ist $\varepsilon$ wie im folgenden entweder 0 oder 1. Wir kommen zu dem etwas komplizierten Fall $\nu \neq 0$, wobei allerdings $\nu = \beta$ noch ausgeschlossen werden muß:

$$R_6 = V^{\lambda} S^{\mu} T S^{\nu} T S^{\alpha} T S^{\beta} T S^{\alpha} V^{-1} S^{-\nu} T^{-1} S^{-\mu} V^{-\lambda}$$
$$= U_{\lambda,\, \mu,\, \nu,\, T} V^{\lambda_*} S^{\mu_*} T S^{\nu_*} S^{\alpha} T S^{\beta} T S^{\alpha} V^{-1} S^{-\nu} T^{-1} S^{-\mu} V^{-\lambda}.$$

Der Kürze halber benutzen wir einige leicht verständliche Abkürzungen und schreiben weiter:

$$R_6 = U_{\mathrm{I}} U^{\varepsilon}_{\lambda_*,\, \mu_*,\, p-1,\, S} U_{\lambda_*,\, \mu_*,\, \nu_*+\alpha,\, T} V^{\overline{\lambda_*+\mathrm{ind}\,(\nu_*+\alpha)}} S^{\overline{\mu_*(\nu_*+\alpha)^2-\nu_*-\alpha}} T S^{(\nu_*+\alpha)_*}$$
$$S^{\beta} T S^{\alpha} V^{-1} S^{-\nu} T^{-1} S^{-\mu} V^{-\lambda}$$
$$= U_{\mathrm{I}} U^{\varepsilon}_{\mathrm{II}} U_{\mathrm{III}} U^{\varepsilon}_{\mathrm{IV}} U_{\overline{\lambda_*+\mathrm{ind}\,(\nu_*+\alpha)},\, \overline{\mu_*(\nu_*+\alpha)^2-\nu_*-\alpha},\, \overline{(\nu_*+\alpha)_*+\beta},\, T}$$
$$V^{\lambda'} S^{\mu'} T S^{\nu'} S^{\alpha} V^{-1} S^{-\nu} T^{-1} S^{\mu} V^{-\lambda}.$$

Wir berechnen $\lambda'$, $\mu'$, $\nu'$, indem wir ihre Bestimmungsgleichungen gemäß (10) aufstellen:

$$\nu' \equiv \frac{-1}{(\nu_*+\alpha)_*+\beta} \pmod p,$$
$$\equiv \frac{-(\nu_*+\alpha)}{-1+\beta(\nu_*+\alpha)}$$
$$\equiv -\frac{\nu_*+\alpha}{\beta\,\nu_*}$$
$$\equiv -\frac{(\nu_*+\alpha)\,\nu\alpha}{\alpha\beta\,\nu\,\nu_*}$$
$$\equiv \nu\alpha^2 - \alpha,$$

$$\mu' \equiv [\mu_*(\nu_*+\alpha)^2 - (\nu_*+\alpha)]\,((\nu_*+\alpha)_*+\beta)^2 - (\nu_*+\alpha)_* - \beta \pmod p$$
$$\equiv \mu_* + \mu_*(\nu_*+\alpha)^2\beta^2 - 2\mu_*(\nu_*+\alpha)\beta - (\nu_*+\alpha)\beta^2 + \beta$$
$$\equiv \mu_*\,\nu_*^2\,\beta^2$$
$$\equiv \mu\,\beta^2,$$

$$\lambda' \equiv \lambda_* + \mathrm{ind}\,(\nu_*+\alpha) + \mathrm{ind}\,((\nu_*+\alpha)_*+\beta) \pmod{\frac{p-1}{2}}$$
$$\equiv \lambda + \mathrm{ind}\,[\nu(\nu_*+\alpha)((\nu_*+\alpha)_*+\beta)]$$
$$\equiv \lambda + \mathrm{ind}\,(-\nu+\nu(\nu_*+\alpha)\beta)$$
$$\equiv \lambda + \mathrm{ind}\,(-\beta)$$
$$\equiv \lambda - 1.$$

Setzt man die gefundenen Werte ein, so findet man:

$$(26)\quad R_6 = U_{\mathrm{I}}\, U_{\mathrm{II}}^{\varepsilon}\, U_{\mathrm{III}}\, U_{\mathrm{IV}}^{\varepsilon}\, U_{\mathrm{V}}\, V^{\lambda-1}\, S^{\overline{\mu\beta^2}}\, T\, S^{\overline{\nu\alpha^2-\alpha}}\, S^{\alpha}\, V^{-1}\, S^{-\nu}\, T^{-1} S^{-\mu}\, V^{-\lambda}$$
$$= U_{\mathrm{I}}\, U_{\mathrm{II}}^{\varepsilon}\, U_{\mathrm{III}}\, U_{\mathrm{IV}}^{\varepsilon}\, U_{\mathrm{V}}\, U^{\varepsilon}_{\overline{\lambda-1},\ \overline{\mu\beta^2},\ p-1,\ S}\, U^{-1}_{\lambda,\ \mu,\ \nu,\ V} = 1 \qquad \nu \neq \beta.$$

Bei dem Fall $\nu = \beta$ begnügen wir uns mit der Angabe des Resultats:

$$(27)\qquad U_{\lambda,\ \mu,\ \beta,\ T}\, U_{\overline{\lambda-1},\ \overline{\mu\beta^2-\beta},\ p-1,\ S}\, U^{\varepsilon}_{\overline{\lambda-1},\ p-1,\ S}\, U^{-1}_{\lambda,\ \mu,\ \beta,\ V} = 1.$$

Die Relationen (23) bis (27) gestatten, die $U_{\mathrm{I}}$ durch die $U_S$ und $U_T$ auszudrücken. Die $U_{\mathrm{I}}$ sind damit eliminiert und die Relationen (23) bis (27) nicht weiter zu berücksichtigen.

## § 5.

## Das Eliminationsverfahren.

Es bleiben demnach noch folgende Erzeugende, die wir in etwas einfacherer Weise bezeichnen wollen:

$$(28)\quad \begin{aligned} (\lambda) &= U_{\lambda,\ p-1,\ S} = V^{\lambda} S^{p} V^{\lambda}, \\ (\lambda,\ \mu) &= U_{\lambda,\ \mu,\ p-1,\ S} = V^{\lambda} S^{\mu} T S^{p} T^{-1} S^{-\mu} V^{\lambda}, \\ (\lambda,\ \mu,\ \nu) &= U_{\lambda,\ \mu,\ \nu,\ T} = V^{\lambda} S^{\mu} T S^{\nu} T S^{-\nu_*} T^{-1} S^{-\mu_*} V^{-\lambda_*} \end{aligned}$$
$$\left(\lambda = 0, 1, \ldots, \frac{p-3}{2};\ \mu = 0, 1, \ldots, p-1;\ \nu = 1, 2, \ldots, p-1\right).$$

Zwischen ihnen bestehen die Relationen:

$$(17\mathrm{a})\qquad (\lambda,\ \mu,\ \nu)\,(\lambda_*,\ \mu_*,\ \nu_*) = 1,$$

$$(19\mathrm{a})\qquad (\lambda,\ \mu,\ 1)\,(\lambda,\ \mu-1) = 1 \qquad \mu \neq 0,$$

$$(20\mathrm{a})\qquad (\lambda,\ 0,\ 1)\,(\lambda,\ p-1)\,(\lambda) = 1,$$

$$(21\mathrm{a})\qquad (\lambda,\ \mu,\ \nu)\,(\lambda_1,\ \mu_1,\ \nu_1)\,(\lambda_2,\ \mu_2,\ \nu_2) = 1 \qquad \nu \neq 1,$$

$$(22\mathrm{a})\qquad (\lambda,\ 0,\ \alpha)\,(\lambda+1,\ p-\alpha)\,(\lambda+1) = 1 \qquad \lambda \neq \frac{p-3}{2}.$$

Unsere Aufgabe ist es nun, ein Verfahren anzugeben, nach dem mit Hilfe obiger Relationen ein Teil der Erzeugenden eliminiert werden kann, während die übrigen ein System unabhängiger Erzeugender bilden. Zu diesem Zweck beginnen wir etwa damit, auf Grund von (19a) und (20a) die $(\lambda,\ \mu)$ durch die $(\lambda,\ \mu,\ 1)$ und $(\lambda)$ auszudrücken. Aus (22a) wird, da $\alpha \neq 1$:

$$(\lambda,\ 0,\ \alpha)\,(\lambda+1,\ p-\alpha+1,\ 1)^{-1}\,(\lambda+1) = 1 \qquad \lambda \neq \frac{p-3}{2}.$$

Diese Relation wird nun benutzt, um alle $(\lambda)$ außer $(0) = S^{p}$ durch die $(\lambda,\ 0,\ \alpha)$ und $(\lambda,\ p-\alpha+1,\ 1)$ auszudrücken. Dann bleiben nur die Re-

lationen (17a) und (21a) übrig. Da gruppentheoretische Relationen $R = 1$, deren linke Seiten dieselbe „zyklische Schreibung" zulassen, nicht wesentlich verschieden sind, so sind in (17a) $\frac{(p-1)^2 p}{4}$ und in (21a) $\frac{(p-2)(p-1)p}{6}$ wesentlich verschiedene Relationen enthalten. Denn man überzeugt sich leicht, daß unter ihnen keine Relationen der Form $(\lambda, \mu, \nu)^2 = 1$ oder $(\lambda, \mu, \nu)^3 = 1$ sich befinden.

Für das Weitere hat man nun folgende vier Fälle zu unterscheiden:

$$\begin{aligned} &\text{I.} && p \equiv -1 \pmod 3, && p \equiv -1 \pmod 4 \\ &\text{II.} && p \equiv -1 \pmod 3, && p \equiv +1 \pmod 4 \\ &\text{III.} && p \equiv +1 \pmod 3, && p \equiv -1 \pmod 4 \\ &\text{IV.} && p \equiv +1 \pmod 3, && p \equiv +1 \pmod 4 \end{aligned}$$

entsprechend der Tatsache[7]), daß $\nu = \nu_*$ für $p \equiv 1 \pmod 4$ zwei Lösungen und $\nu = \nu_1$ für $p \equiv 1 \pmod 3$ zwei Lösungen hat und sonst keine.

Fall I: $p \equiv -1 \pmod{12}$.

Man beachte für das Folgende, daß, wenn $\lambda$ und $\mu$ bei festem $\nu$ ihre zugehörigen Restsysteme durchlaufen, $\lambda_*$ und $\mu_*$ dasselbe tun.

Jedes $(\lambda, \mu, \nu)$ kommt genau einmal in einer binären Relation (17a) vor, ebenso jedes $(\lambda, \mu, \nu)$ außer $(\lambda, \mu, 1)$ genau einmal in einer ternären Relation (21a). Man beginnt daher am besten mit den $(\lambda, \mu, 1)$ und drückt sie mit Hilfe von

$$(\lambda, \mu, 1)\,(\lambda, \mu - 1, p - 1) = 1 \tag{29}$$

durch die $(\lambda, \mu, p-1)$ aus. Dann nimmt man die ternäre Relation, die mit $(\lambda, \mu, p-1)$ beginnt. Sie lautet:

$$(\lambda, \mu, p-1)\,(-, -, 2)\left(-, -, \frac{p+1}{2}\right) = 1. \tag{30}$$

Man eliminiert die $(\lambda, \mu, p-1)$, indem man sie durch die $(\lambda, \mu, 2)$ und die $\left(\lambda, \mu, \frac{p+1}{2}\right)$ ausdrückt. Jetzt sucht man die binären Relationen, in denen $(\lambda, \mu, 2)$ und $\left(\lambda, \mu, \frac{p+1}{2}\right)$ vorkommen. Sie heißen:

$$\begin{aligned} &(\lambda, \mu, 2)\left(-, -, \frac{p-1}{2}\right) = 1, \\ &\left(\lambda, \mu, \frac{p+1}{2}\right)(-, -, p-2) = 1. \end{aligned} \tag{31}$$

Man drückt nun die $(\lambda, \mu, 2)$ durch die $\left(\lambda, \mu, \frac{p-1}{2}\right)$, bzw. die $\left(\lambda, \mu, \frac{p+1}{2}\right)$

[7]) Vgl. [4]).

durch die $(\lambda, \mu, p-2)$ aus und ermittelt die ternären Relationen. in denen diese vorkommen. Sie lauten:

$$\begin{aligned} &\left(\lambda, \mu, \frac{p-1}{2}\right)(-, -, 3)\left(-, -, \frac{2}{3}(p+1)\right) = 1, \\ &(\lambda, \mu, p-2)\left(-, -, \frac{p+3}{2}\right)\left(-, -, \frac{p+1}{3}\right) = 1. \end{aligned} \tag{32}$$

Man eliminiert wie bisher die $\left(\lambda, \mu, \frac{p-1}{2}\right)$ und $(\lambda, \mu, p-2)$ und kommt zu den binären Relationen:

$$\begin{aligned} (\lambda, \mu, 3)\left(-, -, \frac{2p-1}{3}\right) &= 1, \\ \left(\lambda, \mu, \frac{p+3}{2}\right)\left(-, -, \frac{p-2}{3}\right) &= 1, \\ \left(\lambda, \mu, \frac{2}{3}(p+1)\right)\left(-, -, \frac{p-3}{2}\right) &= 1, \\ \left(\lambda, \mu, \frac{p+1}{3}\right)(-, -, p-3) &= 1. \end{aligned} \tag{33}$$

Hier kann es nun, und zwar für $p = 11$ vorkommen, daß die beiden ersten und die beiden letzten Relationen je identisch sind. Für $p = 11$ sind damit alle binären und ternären Relationen aufgebraucht. Als Resultat bleiben die freien Erzeugenden $(\lambda, \mu, 3)$ und $(\lambda, \mu, 5)$. Ebensogut könnte man $(\lambda, \mu, 7)$ und $(\lambda, \mu, 8)$ wählen.

Für $p = 23$ fährt man fort und entnimmt aus (21a) die Relationen:

$$\begin{aligned} \left(\lambda, \mu, \frac{2p-1}{3}\right)(-, -, 4)\left(-, -, \frac{3}{4}(p+1)\right) &= 1, \\ \left(\lambda, \mu, \frac{p-2}{3}\right)\left(-, -, \frac{p+5}{2}\right)(-, -, x) &= 1, \\ \left(\lambda, \mu, \frac{p-3}{2}\right)\left(-, -, \frac{2p+5}{3}\right)(-, -, y) &= 1, \\ (\lambda, \mu, p-3)\left(-, -, \frac{p+4}{3}\right)\left(-, -, \frac{p+1}{4}\right) &= 1. \end{aligned} \tag{34}$$

Die Ausdrücke $x$ und $y$ sind verschieden für Primzahlen, die nicht zum selben Rest mod 5 gehören. Z. B. ist für $p \equiv 3 \pmod 5$, also etwa für 23

$$x = \frac{4p+3}{5}, \quad y = \frac{p+2}{5}.$$

Um den allgemeinen Schritt bei unserem Eliminationsverfahren anzugeben, nehmen wir etwa an, in einer gewissen Anzahl von ternären Relationen kämen nur die Erzeugenden, welche an erster Stelle stehen, nur in diesen vor, d. h, ihre binären Relationen seien schon verbraucht. Dann eliminieren wir diese Erzeugenden und verbrauchen damit die zugehörigen ternären Relationen. Zu den an zweiter und dritter Stelle

stehenden Erzeugenden suchen wir nun die binären Relationen, in denen sie vorkommen. Geben dabei zwei Erzeugende zu derselben binären Relation Anlaß, so eliminieren wir die eine, während die andere als freie Erzeugende übrigbleibt. Alle übrigen Erzeugenden werden durch die in den binären Relationen neu auftretenden Erzeugenden ausgedrückt. Zu diesen neu auftretenden Erzeugenden ermitteln wir nun wieder ihre ternären Relationen. Geben dabei drei Erzeugende zur selben ternären Relation Anlaß, so eliminieren wir die eine, während die beiden anderen als freie Erzeugende übrigbleiben. Geben zwei zur selben ternären Relation Anlaß, so drücken wir die erste durch die zweite und die dritte neu auftretende Erzeugende aus; die zweite Erzeugende bleibt als freie und die dritte zählen wir zu einer neuen Schar neu auftretender Erzeugender. Diese erhalten wir wie oben aus den übrigen ternären Relationen, die ja die oben geforderte Bedingung erfüllen. Wir wiederholen den eben skizzierten Schritt und fahren damit so lange fort, bis alle binären und ternären Relationen verbraucht sind. Daß das Verfahren nicht vorher abbrechen kann, sieht man so ein: erreicht das Verfahren die Erzeugende $(\lambda, \mu, n)$, die in irgendeiner der Reihen (30), (32), (34) usw. der ternären Relationen auftreten möge, so erreicht es auch die Erzeugende $(\lambda, \mu, n+1)$; denn diese kommt entweder in einer früheren Reihe vor oder in derselben wie $(\lambda, \mu, n)$, oder sie tritt in der nächsten Reihe auf, die dann notwendig wird. Z. B. tritt $(\lambda, \mu, 2)$ in (30), $(\lambda, \mu, 3)$ in (32), $(\lambda, \mu, 4)$ in (34) auf. Tritt nun $(\lambda, \mu, 5)$ in den Reihen (30), (32), (34) nicht auf, was für $p > 23$ der Fall sein kann — für $p = 23$ ist $y = 5$ —, so erscheint noch eine weitere Reihe ternärer Relationen, in der $(\lambda, \mu, 5)$ auftritt.

Da mit jeder Relation genau eine Erzeugende eliminiert werden kann, so erhält man die $(\lambda, \mu, n)$ als freie Erzeugende, wo $n$ gerade $\frac{p+1}{6}$ bestimmte Werte annimmt.

Fall II: $p \equiv 5 \pmod{12}$.

Die Bestimmungskongruenz $x^2 \equiv 1 \pmod{p}$ hat für $p \equiv 1 \pmod 4$ zwei Lösungen, nämlich $a \equiv \alpha^{\frac{p-1}{4}}$ und $b \equiv a^3 \equiv \alpha^{\frac{3(p-1)}{4}} \pmod p$. Dabei ist $a + b \equiv a + a^3 \equiv a - a \equiv 0 \pmod p$, folglich $a + b = p$.

Es gibt also jetzt für $\nu$ zwei Werte $a$ und $b$, so daß $a = a_*$ bzw. $b = b_*$. Wir führen deshalb das Eliminationsverfahren wie beim Falle I durch, bis wir auf eine Relation

$$(-, -, a)\,(-, -, a) = 1$$

bzw.

$$(-, -, b)\,(-, -, b) = 1$$

stoßen. Diese lassen wir dann zunächst samt den Erzeugenden $(-, -, a)$ bzw. $(-, -, b)$ beiseite und führen das Verfahren zu Ende. Es liefert die freien Erzeugenden $(\lambda, \mu, n)$, wo $n$ $\frac{p-5}{6}$ bestimmter Werte fähig ist.

Jetzt betrachten wir die Relation:

$$(\lambda, \mu, a)\,(\lambda + \operatorname{ind} a, -, a) = 1.$$

Da $\operatorname{ind} a = \frac{p-1}{4}$, kann man die eine Hälfte der $(\lambda, \mu, a)$ durch die andere etwa auf solche Weise ausdrücken, daß die $(l, \mu, a)$ mit $l = 0, 1, \ldots, \frac{p-5}{4}$ als freie Erzeugende übrigbleiben. Für $b$ bleiben entsprechend die $(l, \mu, b)$ übrig.

Als Beispiel diene $p = 5$. Man wählt $\alpha = 2$ und eliminiert $(-, -, 1)$ durch

$$(-, -, 1)\,(-, -, 4) = 1$$

und $(-, -, 4)$ durch

$$(-, -, 4)\,(-, -, 2)\,(-, -, 3) = 1.$$

Die restlichen binären Relationen

$$(\lambda, \mu, 2)\,(\lambda + 1, 4\mu - 2, 2) = 1,$$

$$(\lambda, \mu, 3)\,(\lambda + 1, 4\mu - 3, 3) = 1$$

benutzt man, um die $(1, \mu, 2)$ bzw. $(1, \mu, 3)$ durch die $(0, \mu, 2)$ bzw. $(0, \mu, 3)$ auszudrücken, so daß diese letzteren als freie Erzeugende übrigbleiben.

Fall III: $p \equiv 7 \pmod{12}$.

Die Kongruenz $x(x-1) \equiv -1 \pmod{p}$ hat nur für $p \equiv 1 \pmod 3$ zwei Lösungen. Wir bestimmen sie, wie folgt:

$$x^2 - x + 1 \equiv 0 \pmod{p}.$$

Da nun

$$x^2 - x + 1 = \frac{x^3 + 1}{x + 1}$$

und $x + p - 1$ sein kann, so folgen aus

$$x^3 \equiv -1 \pmod{p}$$

die beiden Lösungen $c \equiv \alpha^{\frac{p-1}{6}}$ und $d \equiv c^5 \equiv \alpha^{\frac{5(p-1)}{6}}$. Dabei ist

$$c + d \equiv c - c^2 \equiv +1 \pmod{p},$$

folglich $c + d = p + 1$.

Wieder führt unser Verfahren schließlich auf eine ternäre Relation:

$$(\lambda, \mu, c)\,(-, -, c)\,(-, -, c) = 1.$$

Läßt man diese und die entsprechende mit $d$ zunächst beiseite, so liefert das Verfahren die $(\lambda, \mu, n)$ als freie Erzeugende, wo $n$ $\frac{p-7}{6}$ bestimmte Werte annimmt.

Jetzt ist noch die Relation

$$(\lambda, \mu, c)\,(\lambda + \operatorname{ind} c, -, c)\,(\lambda + 2\operatorname{ind} c, -, c) = 1$$

zu betrachten. Da $\operatorname{ind} c = \frac{p-1}{6}$, so läßt sich ein Drittel der $(\lambda, \mu, c)$ auf solche Weise eliminieren, daß etwa die $(l, \mu, c)$ mit $l = 0, 1, \ldots, \frac{p-4}{3}$ als freie Erzeugende übrigbleiben. Entsprechendes gilt für $d$.

Als Beispiel nehmen wir $p = 7$. Man wählt $\alpha = 3$ und findet folgende Relationen:

$$\begin{aligned}
(-, -, 1)\,(-, -, 6) &= 1,\\
(-, -, 6)\,(-, -, 2)\,(-, -, 4) &= 1,\\
(-, -, 2)\,(-, -, 3) &= 1,\\
(-, -, 4)\,(-, -, 5) &= 1,\\
(0, -, 3)\,(1, -, 3)\,(2, -, 3) &= 1,\\
(0, -, 5)\,(2, -, 5)\,(1, -, 5) &= 1.
\end{aligned}$$

Man eliminiert der Reihe nach $(-, -, 1)$, $(-, -, 6)$, $(-, -, 2)$, $(-, -, 4)$, $(2, -, 3)$ und $(2, -, 5)$, so daß als freie Erzeugende bleiben:

$$(0, \mu, 3),\quad (1, \mu, 3),\quad 0, \mu, 5),\quad (1, \mu, 5).$$

Fall IV: $p \equiv 1 \pmod{12}$.

Hier gibt es sowohl ein $a$ und $b$ als auch ein $c$ und $d$. Sie sind alle voneinander verschieden und unterbrechen das Eliminationsverfahren wie im Fall II und Fall III. Dieses liefert unter Beiseitelassung der binären Relationen mit $a$ und $b$ und der ternären mit $c$ und $d$ eine Anzahl freier Erzeugender $(\lambda, \mu, n)$, wo $n$ $\frac{p-13}{6}$ Werte fähig ist. Die binären Relationen mit $a$ und $b$ liefern freie Erzeugende $(l\ \mu, a)$ und $(l, \mu, b)$, wo $l = 0, 1, \ldots, \frac{p-5}{4}$, und die ternären Relationen mit $c$ und $d$ geben freie Erzeugende $(l, \mu, c)$ und $(l, \mu, d)$, wo $l = 0, 1, \ldots, \frac{p-4}{3}$.

Beispiel: $p = 13$. Man kann $\alpha = 2$ nehmen und hat folgende Relationen:

$$\begin{aligned}
(-, -, 1)\,(-, -, 12) &= 1\\
(-, -, 12)\,(-, -, 2)\,(-, -, 7) &= 1\\
(-, -, 2)\,(-, -, 6) &= 1\\
(-, -, 7)\,(-, -, 11) &= 1\\
(-, -, 6)\,(-, -, 3)\,(-, -, 5) &= 1\\
(-, -, 11)\,(-, -, 8)\,(-, -, 9) &= 1\\
(-, -, 3)\,(-, -, 4) &= 1\\
(-, -, 9)\,(-, -, 10) &= 1\\
\hline
(\lambda, -, 5)\,(\lambda + 3, -, 5) &= 1\\
(\lambda, -, 8)\,(\lambda + 3, -, 8) &= 1\\
(\lambda, -, 4)\,(\lambda + 2, -, 4)\,(\lambda + 4, -, 4) &= 1\\
(\lambda, -, 10)\,(\lambda + 4, -, 10)\,(\lambda + 2, -, 10) &= 1.
\end{aligned}$$

Die Reihenfolge der Relationen gibt den Weg der Elimination. Als freie Erzeugende bleiben

$$\begin{aligned}
&(l, \mu, 5), \quad (l, \mu, 8) && l = 0, 1, 2,\\
&(l, \mu, 4), \quad (l, \mu, 10) && l = 0, 1, 2, 3.
\end{aligned}$$

§ 6.

## Das Resultat der Elimination.

In allen vier Fällen hat man $\frac{(p-1)^2 p}{2}$ Erzeugende $(\lambda, \mu, \nu)$, $\frac{(p-1)^2 p}{4}$ binäre und $\frac{(p-2)(p-1)p}{6}$ ternäre Relationen. Da jede Relation zur Elimination einer Erzeugenden dient, so ist die Anzahl der freien Erzeugenden $(\lambda, \mu, \nu)$:

$$\frac{(p-1)^2 p}{2} - \frac{(p-1)^2 p}{4} - \frac{(p-2)(p-1)p}{6} = \frac{(p-1)p(p+1)}{12}.$$

$\nu$ ist dabei, wie man leicht für $p \equiv 1, 5, 7, 12 \pmod{12}$ bestätigt, insgesamt $2\left[\frac{p}{12}\right] + 2$ Werte fähig.

Wir fassen unser Resultat zusammen in folgenden

Satz: Die Hauptkongruenzgruppe $p$-ter Stufe ist für $p > 3$ freie Gruppe von $1 + \frac{(p-1)p(p+1)}{12}$ Erzeugenden. Diese sind außer $S^p$ so wählbar, daß sie sich in folgender Form schreiben lassen:

$$(\lambda, \mu, \nu) = V^{\lambda} S^{\mu} T S^{\nu} T S^{-\nu_*} T S^{-\mu_*} V^{-\lambda_*}.$$

$\nu$ $(\neq 0, \neq 1, \neq p-1)$ kann $2\left[\frac{p}{12}\right] + 2$ explizit nicht angebbare, durch

ein Eliminationsverfahren berechenbare Werte annehmen, $\mu$ durchläuft die Zahlen 0 bis $p-1$ und $\lambda$ im allgemeinen die Zahlen 0 bis $\frac{p-3}{2}$. Bei $p \equiv 1 \pmod 4$ jedoch gibt es für $\nu$ zwei Werte $a$ und $b$, für welche $\lambda$ nur bis $\frac{p-5}{4}$ laufen muß. Ebenso gibt es bei $p \equiv 1 \pmod 3$ für $\nu$ zwei Werte $c$ und $d$, für welche $\lambda$ nur bis $\frac{p-4}{3}$ laufen muß. Die $\lambda_*, \mu_*, \nu_*$ ermitteln sich aus (10).

In der oben genannten Arbeit von Rademacher werden die Erzeugenden derjenigen Kongruenzuntergruppen bestimmt, deren Nebengruppenrepräsentanten $E = 1, TS^\nu$ $(\nu = 0, 1, \ldots, p-1)$ sind. Erweitert man die Hauptkongruenzgruppen mit den am Ende von § 1 genannten Untergruppen der Modulargruppen, so kommt man gerade auf diese Kongruenzuntergruppen. Nimmt man daher zu obigen Erzeugenden noch $S$ und $V$ hinzu, so ergibt eine leichte Überlegung das Resultat von Rademacher.

Wir geben eine kurze Zusammenstellung der freien Erzeugenden bis $p = 23$. Dabei werden auch die besonders zu behandelnden Fälle $p = 2$ und $p = 3$ aufgeführt.

$p = 2$: $(0) = S^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $(0, 0) = TS^2T = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$[8];

$p = 3$: $(0) = S^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$, $(0, 0) = TS^3T = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}$,

$$(0, 1) = STS^3TS^{-1} = \begin{pmatrix} -2 & 3 \\ -3 & 4 \end{pmatrix};$$

$p = 5, 7, 11, 13$: siehe oben § 5;

$p = 17$: $(0) = S^{17}$

$(\alpha = 3)$ $(\lambda, \mu, 5)$, $(\lambda, \mu, 7)$, $\lambda = 0$ bis 7; $(l, \mu, 4)$, $(l, \mu, 13)$, $l = 0, 1, 2, 3$ } $\mu = 0$ bis 16;

$p = 19$: $(0) = S^{19}$

$(\alpha = 2)$ $(\lambda, \mu, 4)$, $(\lambda, \mu, 5)$, $\lambda = 0$ bis 8; $(l, \mu, 8)$, $(l, \mu, 12)$, $l = 0$ bis 5 } $\mu = 0$ bis 18;

$p = 23$: $(0) = S^{23}$

$(\alpha = 5)$ $(\lambda, \mu, 4)$, $(\lambda, \mu, 5)$, $(\lambda, \mu, 6)$, $(\lambda, \mu, 14)$,
$\lambda = 0$ bis 10; $\mu = 0$ bis 22.

---

[8]) $\mathfrak{G}^{(2)}$ ist die Diedergruppe der Ordnung 6. Es ist bemerkenswert, daß die Modulgruppe noch einen anderen freien Normalteiler vom Index 6 aus zwei Erzeugenden besitzt: die Kommutatorgruppe, die von den Elementen $TSTS^{-1}$ und $S^{-1}TST$ erzeugt wird. Vgl. § 7. Der Durchschnitt der beiden Gruppen ist der von der Klasse der zu $S^{-2}TS^2T$ innerhalb $\Gamma_2$ konjugierten Elemente erzeugte Normalteiler.

Die Art der errechneten freien Erzeugenden hängt ab von der speziellen Wahl der Nebengruppenrepräsentanten (4), von der Wahl von $\alpha$ und insbesondere von unserem Eliminationsverfahren. Doch muß jedes andere mögliche System von Erzeugenden aus dem angegebenen durch einen Automorphismus hervorgehen. Die Erzeugenden wären z. B. von geringerer Länge, wenn man die Nebengruppenrepräsentanten so festlegen würde, daß in (4) für $V^\lambda$ das damit kongruente Wort $TS^{\alpha^\lambda}TS^{\beta^\lambda}TS^{\alpha^\lambda}$ genommen wird, und die Exponenten von $S$ in (4) dann mod $p$ auf positive Zahlen $< p$ reduziert werden. Diese Wahl der Repräsentanten hätte den Vorteil, daß sie die Forderung $(F)$ erfüllen würde, so daß die Relationen (22a) wegfielen und die übrigen einige Modifikationen erführen. Andererseits wären dann die Erzeugenden $(\lambda, -\alpha^\lambda, -\beta^\lambda)$ für $\lambda \neq 0$ mit der Einheit identisch, was eine nicht unerhebliche Komplizierung des Eliminationsverfahrens zur Folge hätte. Bei der getroffenen Wahl der Nebengruppenrepräsentanten hat das oben angegebene Eliminationsverfahren den Vorteil großer Durchsichtigkeit für den allgemeinen Fall, aber den Nachteil, daß es die freien Erzeugenden zum Teil in komplizierterer Form als nötig liefert. Denn es eliminiert z. B. die einfacher gebauten Erzeugenden $(\lambda)$ und $(\lambda, \mu)$, die Transformierte von $S^\mu$ sind.

## § 7.

## Ein allgemeiner Satz über Erzeugendenanzahlen.

Wir wollen zeigen, wie die Anzahl der freien Erzeugenden ohne deren explizite Aufstellung mit Hilfe des Schreierschen Verfahrens ermittelt werden kann. Die dabei nötige Überlegung ist nicht auf den Fall der Modulgruppe beschränkt. Wir gehen daher allgemein vor.

Eine Gruppe $\mathfrak{G}$ werde erzeugt durch die Elemente $A_\varrho$ $(\varrho = 1, 2, \ldots, k)$ und $B_\sigma$ $(\sigma = 1, 2, \ldots, m)$ mit den Relationen $A_\varrho^{a_\varrho} = 1$. $\mathfrak{G}$ besitze eine Untergruppe $\mathfrak{U}$ von endlichem Index $j$ mit den Nebengruppenrepräsentanten $\overline{G}$, die die Schreiersche Forderung $(F)$ erfüllen mögen. Die Erzeugenden von $\mathfrak{U}$ sind

$$U_{\overline{G}, A_\varrho} = \overline{G} A_\varrho G A_\varrho^{-1} \quad \text{und} \quad U_{\overline{G}, B_\sigma} = \overline{G} B_\sigma \overline{G B}_\sigma^{-1}.$$

Die Anzahl derjenigen $U$, die nicht $\equiv 1$ sind, sei mit Schreier[9]) ermittelt zu

$$Z = 1 + (k + m - 1)j. \tag{35}$$

Die Relationen, denen die $U$ noch gehorchen, lauten

$$\overline{G} A_\varrho^{a_\varrho} \overline{G}^{-1} = 1.$$

[9]) A. a. O., § 4.

Ist nun $A_\varrho^{t_\varrho}$ die niederste Potenz von $A_\varrho$, die in $\mathfrak{U}$ liegt ($t_\varrho$ ist Teiler von $a_\varrho$), so lassen sich die letzteren umschreiben in folgende Relationen der $U$, von denen einige, ohne die Überlegung zu stören, $= 1$ sein können:

$$(36) \qquad \left[\prod_{i=0}^{t_\varrho - 1} (\overline{G}_{i,\varrho} A_\varrho \overline{G}_{i+1,\varrho}^{-1})\right]^{\frac{a_\varrho}{t_\varrho}} = 1.$$

Denn wird $\overline{G}_{0,\varrho} = \overline{G}$, $\overline{G}_{i+1,\varrho} = \overline{G_{i,\varrho} A_\varrho}$ gesetzt, so folgt $\overline{G}_{t_\varrho,\varrho} = \overline{G}$. Es kann nun vorkommen, daß $\overline{G}_{i,\varrho} = \overline{G}_{i+1,\varrho}$. Dann geht (36) über in

$$(37) \qquad (\overline{G} A_\varrho \overline{G}^{-1})^{a_\varrho} = 1,$$

und Relationen dieser Art gibt es genau so viele, als es Transformierte von $A_\varrho$ in $\mathfrak{U}$ gibt. Ist ihre Anzahl $z_\varrho$ und nimmt man der Einfachheit halber des weiteren $t_\varrho = a_\varrho$ [10]), so sind mit (36) außer (37) noch $\frac{j - z_\varrho}{a_\varrho}$ Relationen gemeint. Jede dient dazu, gerade noch je eine Erzeugende zu eliminieren. Man hat also das Resultat:

Satz: Besitzt die Gruppe $\mathfrak{G}\{A_\varrho (\varrho = 1, \ldots, k),\ B_\sigma (\sigma = 1, \ldots, m);\ A_\varrho^{a_\varrho} = 1\}$ eine Untergruppe $\mathfrak{U}$ von endlichem Index $j$, in der keine (außer der $a_\varrho$-ten) Potenz der $A_\varrho$ vorkommt, so wird $\mathfrak{U}$ erzeugt von

$$Z = 1 + (k + m - 1) j - \sum_{\varrho=1}^{k} \frac{j - z_\varrho}{a_\varrho}$$

Elementen. $z_\varrho$ ist die Anzahl der Transformierten von $A_\varrho$ in $\mathfrak{U}$, und $\mathfrak{U}$ gehorcht nur der Bedingung, daß diese Transformierten die Ordnung $a_\varrho$ haben. $\mathfrak{U}$ ist also frei, wenn $z_\varrho = 0$, was insbesondere für einen Normalteiler zutrifft.

Die damit gegebene Abzählung der Erzeugenden läßt nun entsprechend wie die für freie Gruppen von Schreier angegebene Beziehung (35) eine geometrisch anschauliche Bestätigung zu [11]). Wir zeigen das etwa für einen Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$. Statt des von Schreier benutzten Dehnschen Gruppenbildes wählt man in diesem Falle sachgemäßer das der Modulteilung entsprechende Klein-Dycksche Gruppenbild [12]). Der „halbe“

[10]) Ist $t_\varrho \neq a_\varrho$, so lassen sich die in (37) nicht aufgezählten Relationen von (36) durch geeignete Automorphismen auf die Form bringen: $U^{\frac{a_\varrho}{t_\varrho}} 1$. Dieser Sachverhalt entspricht einem Satz, den mir Herr Prof. Reidemeister gesprächsweise mitgeteilt hat: Die Untergruppen eines freien Produktes zyklischer Gruppen sind wieder freie Produkte zyklischer Gruppen.

[11]) Folgende Überlegung verdanke ich einer freundlichen Anregung von Herrn Prof. Reidemeister (Königsberg).

[12]) Vgl. etwa die unter Fußnote [6]) zitierte Arbeit von v. Dyck.

Fundamentalbereich von $\mathfrak{G}$ besteht demnach aus einem von Kreisen, die alle auf einer und derselben Geraden senkrecht stehen, gebildeten Kreisbogen-$(k+m+1)$-Eck mit den Winkeln $\pi/a_\varrho$ an den Ecken, die den $A_\varrho$ entsprechen, und den Winkeln 0 an den übrigen Ecken, die den $B_\sigma$ entsprechen, und einem weiteren homogenisierenden Element $C$, für welches gilt:

$$\left(\prod_{\varrho=1}^{k} A_\sigma\right)\left(\prod_{\sigma=1}^{m} B_\sigma\right)C = 1.$$

Man denke sich nun das Dycksche Bild ausgeführt.

Der Faktorgruppe $\mathfrak{F} = \mathfrak{G}/\mathfrak{N}$ ist als Bild zugeordnet eine Gesamtheit von $2j$ Polygonen, die etwa einen einfach zusammenhängenden Bereich erfüllen, dessen Ränder paarweise zusammengehören. Dieser Bereich ist ein Fundamentalbereich für $\mathfrak{N}$, seine Ränderzuordnungen ergeben Erzeugende von $\mathfrak{N}$. Sind die Ränder zusammengefügt, so entsteht eine Fläche $F$ vom Geschlecht $P$. Den (unabhängigen) Schnitten, die nötig sind, um aus dieser Fläche den Fundamentalbereich von $\mathfrak{N}$ zu erhalten, entsprechen die freien Erzeugenden von $\mathfrak{N}$.

Zur Ermittelung der Anzahl dieser Schnitte bemerken wir, daß den $B_\sigma$ in $\mathfrak{F}$ die Ordnung $b_\sigma$ und $C$ die Ordnung $c$ zukommen soll und daß eine Ecke auf $F$, in der $2e$ Polygone zusammenstoßen, „Punkt vom Typus $e$" heißen soll. Wegen regulärer Aufteilung liegen auf $F$ genau $j/e$ Punkte vom Typus $e$. Man schneidet nun zunächst längs der $2P$ auf $F$ möglichen Rückkehrschnitte auf. Diese Schnitte sollen längs Polygonseiten verlaufen und alle etwa in einem und demselben Punkte vom Typus $c$ beginnen und enden; im übrigen sollen die Schnitte die Punkte vom Typus $b_\sigma$ und $c$ meiden, und die Schnittwege sind im topologischen Sinne als nicht über sie hinwegziehbar zu verstehen. Nachdem so der Zusammenhang von $F$ ein einfacher geworden ist, genügt es, noch Schnitte bis zu den übrigen Punkten vom Typus $b_\sigma$ und $c$ zu ziehen bzw. sie mit einem bereits vorhandenen Ufer zu verbinden. Diesen Schnitten entsprechen als Erzeugende Transformierte von $B_\sigma^{b_\sigma}$ und $C^c$. Man findet daher für $Z$:

$$Z = 2P - 1 + \sum_{\sigma=1}^{m} \frac{j}{b_\sigma} + \frac{j}{c},$$

woraus mit Hilfe der Geschlechtsformel

$$2P - 2 = j\left[(k+m-1) - \sum_{\varrho=1}^{k} \frac{1}{a_\varrho} - \sum_{\sigma=1}^{m} \frac{1}{b_\sigma} - \frac{1}{c}\right]$$

folgt

$$Z = 1 + (k+m-1)j - \sum_{\varrho=1}^{k} \frac{j}{a_\varrho}.$$

Man kann diesen Sachverhalt auch so ausdrücken:

$\mathfrak{N}$ ist holoedrisch isomorph mit der Wegegruppe der zu $\mathfrak{F} = \mathfrak{G}/\mathfrak{N}$ gehörenden geschlossenen Fläche, wenn diese „punktiert" ist in denjenigen Punkten, deren Typus (Verzweigungscharakter) gegenüber $\mathfrak{G}$ verändert ist.

Daß eine der genannten Transformierten als Erzeugende entfallen muß, hat seinen Grund in der topologischen Tatsache, daß ein Weg, der alle Punktierungen umschließt, dem bekannten im Falle der Nichtpunktierung mit der Einheit identischen Produkt der Rückkehrschnitte gleichkommt, was nicht zur Elimination eines Rückkehrschnitts benutzt werden kann, weil jeder Rückkehrschnitt in diesem Produkt zweimal vorkommt.

Der Fall der Hauptkongruenzgruppe ordnet sich mit $A_1 = T$, $A_2 = TS^{-1}$ dem allgemeinen Resultat unter und liefert (für eine beliebige Stufe $n$):

$$Z = 1 + \frac{g}{6}.$$

Zugleich sieht man, weshalb ein Eliminationsverfahren, das die an sich einfacheren Erzeugenden $(\lambda)$ und $(\lambda, \mu)$ nicht eliminiert, ungünstig ist. Denn dann ist die Aufstellung der Relation, die nach obigem das Produkt aller $(\lambda)$ und $(\lambda, \mu)$ mit den $(\lambda, \mu, \nu)$ verbindet, unvermeidlich, was zum mindesten sehr umständlich ist.

Auch die von Rademacher für die von ihm untersuchten Untergruppen angegebenen Anzahlen lassen sich rasch aus obigem Satze ableiten.

## § 8.

## Die Modulargruppe abstrakt.

Solange $I' = 0$, lassen sich die Erzeugenden als Transformierte von $S^p$ wählen. Das ist wegen

$$P = 1 + \frac{(p^2 - 1)\,(p - 6)}{24}$$

nur für $p \leqq 5$ möglich. Dasselbe folgt unabhängig von den Überlegungen des § 7 aus der Tatsache, daß dann die Anzahl der $(\lambda)$ und $(\lambda, \mu)$ nicht kleiner sein darf als die Zahl der verlangten freien Erzeugenden. Es sei daher für $p = 5$ noch eine andere Elimination angegeben, die zugleich die Umständlichkeit dieses Weges dartut. Die ursprünglichen Eliminationsrelationen lassen sich nach Elimination von $(\lambda, \mu, 1)$ so schreiben:

$$(38)\qquad \begin{aligned} (\lambda, \mu, 4) &= (\lambda + 1, \mu) && \mu \neq 4, \\ (\lambda, 4, 4) &= (\lambda + 1, 4)\,(\lambda), \end{aligned}$$

$$(39)\qquad (\lambda, \mu, 2)\,(\lambda + 1, 4\mu - 2, 2) = 1,$$

$$(40)\qquad (\lambda, \mu - 1, 3)\,(\lambda + 1, 4\mu - 2, 3) = 1,$$

$$(41)\qquad (\lambda, \mu, 2)\,(\lambda + 1, 4\mu - 2, 3)\,(\lambda, \mu - 1, 4) = 1,$$

$$(42)\qquad (0, 0, 2)\,(1, 3)\,(1) = 1.$$

Man drückt mit Hilfe von (39) und (40) die $(1, \mu, 2)$ bzw. $(1, \mu, 3)$ durch die $(0, \mu, 2)$ bzw. $(0, \mu, 3)$ aus. Aus (41) wird dann:

$$(43) \qquad (0, \mu, 2)\,(0, \mu - 1, 3)^{-1}\,(0, \mu - 1, 4) = 1$$

und

$$(44) \qquad (0, 4\mu - 2, 2)^{-1}\,(0, 4\mu - 2, 3)\,(1, \mu - 1, 4) = 1.$$

Statt (44) läßt sich auch schreiben:

$$(45) \qquad (0, \mu - 1, 2)^{-1}\,(0, \mu - 1, 3)\,(1, 4\mu - 2, 4) = 1.$$

Aus (43) und (45) folgt bei Elimination von $(0, \mu, 3)$:

$$(46) \qquad (0, \mu, 2)\,(1, 4\mu - 2, 4)\,(0, \mu - 1, 2)^{-1}\,(0, \mu - 1, 4) = 1.$$

(46) gestattet, $(0, \mu, 2)$ durch $(0, \mu - 1, 2)$ und $(\lambda, \mu, 4)$ auszudrücken. Führt man das der Reihe nach für $\mu = 1, 2, 3, 4, 0$ durch und setzt das jeweilige Resultat in das folgende ein, so kommt eine Relation zum Vorschein, in der $(0, 0, 2)$ zweimal und jedes $(\lambda, \mu, 4)$ genau einmal vorkommt. Unter Berücksichtigung von (38) und (42) geht sie über in die Relation zwischen den $(\lambda)$ und $(\lambda, \mu)$, von der am Ende von § 7 die Rede war. Man benutzt sie, um etwa noch $(1, 4)$ zu eliminieren. Die dann noch bleibenden Erzeugenden lassen sich mit Hilfe geeigneter Automorphismen auf die Form bringen:

$$S^5, \quad S^\mu T S^5 T S^{-\mu}, \quad S^\mu T S^3 T S^5 T S^{-3} T S^{-\mu} \qquad \mu = 0, 1, 2, 3, 4.$$

Will man die Modulargruppe abstrakt charakterisieren, d. h. durch Angabe hinreichender und womöglich unabhängiger Relationen $R(S, T) = 1$, so hat man dazu nur die Erzeugenden von $\Gamma$ der Einheit gleichzusetzen.

$$(47) \qquad S^p = T^2 = (S T)^3 = 1$$

reicht nur für $p = 2$ (Diedergruppe der Ordnung 6), $p = 3$ (Tetraedergruppe), $p = 5$ (Ikosaedergruppe) aus. Für $p \geqq 7$ müssen zu (47) mindestens eine, höchstens $2P$ weitere Relationen hinzutreten. Diese Höchstzahl läßt sich aber noch erheblich reduzieren.

Da $(\lambda, \mu, \nu)$ sich als Transformierte von $(0, \mu, \nu)$ auffassen läßt, so genügen also nach § 6, wenn die Exponenten von $S$ mod $p$ verstanden werden, neben (47) die Relationen

$$(48) \qquad S^\mu T S^\nu T S^{1/\nu} T S^{\nu - \mu\nu^2} = V^{\mathrm{ind}\,\nu} \qquad \nu \neq 0, \pm 1,$$

$$(49) \qquad V^{\frac{p-1}{2}} = 1$$

zur Charakterisierung der Modulargruppe. (48) und (49) sind aber gleichbedeutend mit

$$(50) \qquad S^\mu T S^\nu T S^{1/\nu} T S^{-\mu\nu^2} T S^{-1/\nu} T S^{-\nu} T = 1$$

und

$$(51) \qquad V^{\mathrm{ind}\,\nu} = T S^\lambda T S^{1/\nu} T S^\nu.$$

Aus (50) folgt für $\mu = 1$, $\nu = \alpha$:

$$V^{-1} S V = S^{\alpha^2}$$

und daraus

$$V^{-r} S^{\alpha^\varepsilon} V^r = S^{\alpha^{2r+\varepsilon}} \quad \text{für} \quad \varepsilon = 1, 0, -1. \tag{52}$$

Setzt man $V_\nu \equiv T S^\nu T S^{1/\nu} T S^\nu$, so folgt aus (49) bis (51):

$$\begin{aligned} V_\nu T &= T T S^{1/\nu} T S^\nu T S^{1/\nu}, \\ &= T V^{\text{ind } 1/\nu}, \\ &= T (V^{\text{ind } \nu})^{-1} \end{aligned}$$

oder

$$(V_\nu T)^2 = 1. \tag{53}$$

Es läßt sich nun zeigen, daß (50) und (51) aus (53) folgt. Zunächst sei (51) als Folge von (50) und (53) dargestellt, indem man (52), das ja aus (50) folgt, dazu benutzt, die rechte Seite von (51) in Potenzen von $V$ auszudrücken. Wir nehmen $\nu = \alpha^{2r+\varepsilon}$ und formen mit Hilfe von $(V T)^2 = 1$ um:

$$\begin{aligned} T S^\nu T S^{1/\nu} T S^\nu &= T V^{-r} S^{\alpha^\varepsilon} V^r T V^r S^{\alpha^{-\varepsilon}} V^{-r} T V^{-r} S^{\alpha^\varepsilon} V^r \\ &= T V^{-r} S^{\alpha^\varepsilon} T S^{\alpha^{-\varepsilon}} T S^{\alpha^\varepsilon} V^r \\ &= T V^{-r} T V^\varepsilon V^r \\ &= V^{2r+\varepsilon} \\ &= V^{\text{ind } \nu}. \end{aligned}$$

Zum Nachweis, daß (50) eine Folge von (53) ist, bezeichnen wir die linke Seite von (50) mit $R_\mu$ und finden:

$$R_{m+\mu} = S^m R_\mu S^{-m} R_m.$$

Ist darin nun $m$ fest und $\neq 0$ und läßt man $\mu$ der Reihe nach die Werte $m, 2m, \ldots, (p-1)m$ annehmen, so sieht man, daß es genügt, $R_m = 1$ zu setzen. Wählt man $m = 2/\nu$, so erkennt man $R_m = 1$ rasch als Folge von $(V_\nu T)^2 = (V_{1/\nu} T)^2 = 1$.

Statt (53) schreibt man besser

$$(S^{2\nu} T S^{1/\nu} T)^2 = 1 \tag{54}$$

und hat also das Ergebnis [13]):

---

[13]) das in der Form (54) von Bussey stammt [Proc. Lond. Math. Soc. (2), **5** (1905), S. 296]. Andere hinreichende Relationen hat zuerst Moore angegeben. Vgl. auch Dickson (Proc. Lond. Math. Soc. **35**, S. 292) oder „Linear groups" (1901), S. 300. In neuerer Zeit gab B. Malmrot dieselbe Charakterisierung der Modulargruppe im 2. Teil seiner Dissertation: „Studien über Gruppen, deren Ordnung ein Produkt von 6 Primzahlen ist", Uppsala 1925 (zitiert nach Fortschritte der Math. Jahrgang 1925).

Die Modulargruppe $p$-ter Stufe ist charakterisiert durch (47) und (54), wo $\nu$ nur eine gewisse Anzahl von Werten $< \frac{1}{2}(p-1)$ anzunehmen hat. Denn erstens geben die Werte $\nu$, $-\nu$, $\frac{1}{2\nu}$, $-\frac{1}{2\nu}$ zur selben Relation (54) Anlaß. Zweitens läßt sich die Herleitung von (54) ebenso durchführen, wenn $\nu$ nur die Werte $\alpha, \beta$ und die durch das Eliminationsverfahren von § 5 gefundenen Werte und ihre Reziproken annimmt.

Wir geben eine Zusammenstellung der abstrakten Modulargruppen bis $p = 23$, wobei die Relation $(S^x T S^y T)^2 = 1$ durch $(x, y)$ symbolisiert sei:

$$S^p = T^2 = (ST)^3 = 1,$$

$p = 7$: $(3, 3)$ [14]),

11: $(4, 6)$ [15]),

13: $(3, 5)$ $(4, 7)$,

17: $(3, 12)$ $(4, 9)$ $(6, 6)$ [16]),

19: $(3, 7)$ $(4, 10)$ $(5, 8)$,

23: $(4, 12)$ $(5, 5)$ $(6, 8)$ $(9, 13)$.

Auf eine durchsichtigere Weise läßt sich die Modulargruppe durch die Erzeugenden $S$, $T$, $V$ so charakterisieren:

$$S^p = V^{\frac{p-1}{2}} = T^2 = (ST)^2 = (VT)^2 = 1, \quad V^{-1} S V = S^{\alpha^2}.$$

Schließlich sei noch bemerkt, daß sich aus (50) und (53) leicht bestätigen läßt

$$(S^\nu T S^{1/\nu} T)^3 = 1.$$

Doch bleibe es dahingestellt, ob diese Relationen zur Charakterisierung ausreichen.

---

[14]) Vgl. v. Dyck a. a. O., S. 41 und Burnside „The Theory of Groups" (1911), S. 422.

[15]) Die von Dickson [Americ. M. S. Bull. (2) 9, S. 204] aufgeführte weitere Relation (3, 8) ist entbehrlich.

[16]) Die außerdem noch errechnete Relation (7, 10) ist eine Folge der übrigen.

(Eingegangen am 23. 5. 1932).

# Lebenslauf.

Ich, Hermann Karl Friedrich Frasch, Sohn des Eisenbahnoberinspektors in Jagstfeld, Hermann Frasch und seiner Ehefrau Pauline geb. Luz, bin am 21. Juni 1906 zu Stuttgart geboren. Ich besuchte von 1912 bis 1917 das Gymnasium zu Ludwigsburg von 1917 bis 1920 das Progymnasium zu Oehringen. 1920 bestand ich das württembergische evangelische Landexamen und besuchte dann je zwei Jahre die theologischen Seminare Schöntal und Urach. An letzterem legte ich 1924 die Reifeprüfung ab.

In den Jahren 1924 bis 1929 studierte ich Mathematik und Physik an den Universitäten Tübingen (zwei Semester), Hamburg (zwei Semester), Göttingen (ein Semester), Tübingen (fünf Semester). Meine akademischen Lehrer waren in Tübingen die Herren Professoren Back, Gerlach, Hessenberg †, Kamke, Knopp, Kommerell, Landé, Maurer †, Paschen, Rosenberg, Schönhardt, Thierfelder †; in Hamburg die Herren Artin, Blaschke, Hecke, Koch; in Göttingen die Herren Bessel-Hagen, Hertz, Hilbert, Landau, Fräulein Noether.

Im Frühjahr 1929 legte ich die erste, im Frühjahr 1930 die zweite württembergische Dienstprüfung für das höhere Lehramt ab. Dann war ich bis Ostern 1931 im Schuldienst tätig. Seit dieser Zeit bin ich ohne Anstellung.